Nations Unies A/56/164

Assemblée générale

Distr. générale
3 juillet 2001
Français
Original: anglais/espagnol

Cinquante-sixième session
Point 81 de la liste préliminaire*
Les progrès de la téléinformatique dans le contexte de la sécurité internationale

Les progrès de la téléinformatique dans le contexte de la sécurité internationale

Rapport du Secrétaire général

Table des matières

Page

I. Introduction 2
II. Réponses reçues des gouvernements 2
Bolivie 2
Mexique 2
Philippines 4
Suède** 6

* A/56/50.
** Au nom des États membres de l'Union européenne qui sont membres de l'Organisation des Nations Unies.

01-44867 (F) 090801 100801
0144867

I. Introduction

1. Dans sa résolution 55/28 du 20 novembre 2000 consacrée aux progrès de la téléinformatique dans le contexte de la sécurité internationale, l'Assemblée générale a invité tous les États Membres à continuer de communiquer au Secrétaire général leurs vues et observations sur les questions suivantes : a) les problèmes généraux en matière de sécurité de l'information; b) la définition des concepts fondamentaux en matière de sécurité de l'information, notamment les interférences illicites dans les systèmes télématiques ou l'utilisation illégale de ces systèmes; c) la teneur des principes internationaux visant à renforcer la sécurité des systèmes télématiques mondiaux; et a prié le Secrétaire général de lui présenter, en s'appuyant sur les réponses reçues des États Membres, un rapport à ce sujet à sa cinquante-sixième session.

2. Le 19 mars 2001, le Secrétaire général adressait une note verbale aux États Membres par laquelle il les priait, à la demande de l'Assemblée, de lui faire part de leurs observations. On trouvera à la section II du présent rapport les réponses reçues des gouvernements au 3 juillet 2001. Toute autre réponse reçue ultérieurement sera publiée sous forme d'additif.

II. Réponses reçues des gouvernements

Bolivie

[Original : espagnol]
[14 juin 2001]

Selon l'information reçue de la Chancellerie bolivienne, les forces armées boliviennes ne disposent pas à l'heure actuelle de ressources électroniques appropriées et ne prévoient pas d'en faire l'acquisition ni d'en fabriquer à l'avenir.

Mexique

[Original : espagnol]
[16 mai 2001]

1. Le Mexique estime qu'il faut redoubler d'efforts pour encourager les applications civiles des progrès scientifiques et techniques et des technologies de l'information. Il a soutenu les résolutions 53/70 du 4 décembre 1998 et 54/49 du 1er décembre 1999 que l'Assemblée générale a consacrées aux progrès de la téléinformatique dans le contexte de la sécurité internationale.

2. À l'heure actuelle, les principales difficultés tiennent à la vulnérabilité possible des systèmes d'information sur lesquels reposent les programmes de défense de certains pays et au risque que les technologies de l'information et des communications soient utilisées par des terroristes ou servent à exercer des pressions.

3. Dans cette optique, la coopération internationale et le droit international offrent la seule voie pour éviter que les mesures adoptées pour faire face aux problèmes posés par la sécurité de l'information ne restreignent de quelque façon que ce soit la liberté d'information et de communication.

4. Il s'agit là d'une question importante. On devra cependant tenir compte des travaux et des avancées des autres comités de l'Assemblée générale, puisqu'ils pourraient faciliter grandement la définition de notions de nature à être prises en compte dans le cadre de l'examen des problèmes que pose la sécurité de l'information.

5. En ce qui concerne la définition de critères ou concepts internationaux fondamentaux relatifs à la sécurité de l'information, le Mexique estime que la notion d'interférence illicite peut prêter à confusion, dans la mesure où elle fait penser à des activités entreprises par certains pays qui, au nom de raisons humanitaires discutables ou pour d'autres motifs, interviennent soit à titre individuel soit de manière concertée dans les affaires d'autres États.

6. Il serait donc préférable de préférer à cette notion celle d'« accès non autorisé » ou simplement d'« accès illicite » pour désigner les activités auxquelles se livrent certains individus ou certaines entités s'agissant des systèmes d'information.

7. En ce qui concerne la nécessité d'arrêter des principes internationaux de nature à renforcer la sécurité des systèmes télématiques mondiaux, il importe de souligner que ces principes ne doivent pas seulement viser à améliorer la sécurité des systèmes mais aussi à la garantir plus efficacement par la voie juridique.

8. On devrait également examiner minutieusement les dispositions pertinentes contenues dans les instruments internationaux adoptés au fil des ans tant par l'Assemblée générale des Nations Unies que par d'autres organisations internationales – notamment l'Organisation des Nations Unies pour l'éducation, la science et la culture (UNESCO) – s'agissant de la sécurité internationale, du terrorisme international et de l'information, dans un souci de recenser et d'évaluer les principes existant en la matière.

9. À cet effet, le Mexique appuie la résolution 51/210 de l'Assemblée générale, du 17 décembre 1996, relative aux mesures visant à éliminer le terrorisme international, notamment l'alinéa c) du paragraphe 3 (partie I), lequel a trait aux risques que comporte l'utilisation par des terroristes des réseaux et des systèmes télématiques en vue de commettre des actes criminels et à la nécessité de trouver des moyens, conformes au droit national, pour prévenir de tels actes et promouvoir, si nécessaire, une coopération.

10. Pendant le dixième Congrès des Nations Unies pour la prévention du crime et le traitement des délinquants, qui s'est tenu à Vienne du 10 au 17 avril 2000, le Secrétariat a présenté un document intitulé « Délits liés à l'utilisation du réseau informatique » (A/CONF.187/10), dans lequel il appelait l'attention sur le fait que pour prévenir et combattre efficacement la criminalité informatique, une action mondiale coordonnée s'imposait à différents niveaux.

11. Au niveau national, enquêter sur la criminalité informatique exige du personnel et des connaissances spécialisés et des procédures adéquates. Il serait souhaitable que les États envisagent d'établir des mécanismes qui permettent d'obtenir au moment opportun des données fiables provenant des systèmes et des réseaux informatiques, lorsque ces données doivent servir de preuves dans des procédures judiciaires.

12. Au niveau international, enquêter efficacement sur la criminalité informatique signifie intervenir au moment opportun, en coordination avec les services chargés de l'application des lois et l'autorité juridique compétente.

Philippines

[Original : anglais]
[22 mai 2001]

1. Problèmes généraux en matière de sécurité de l'information

1. La sécurité de l'information est une question cruciale, qui revêt une dimension mondiale du fait de la complexité et de l'étendue des problèmes qu'elle suscite. Les risques qui l'accompagnent se propagent rapidement en cette ère de l'information. Le moindre progrès technologique, la moindre innovation peuvent d'ailleurs être retournés contre l'humanité.

2. Les problèmes qui existent en matière de sécurité de l'information sont comparables à la menace que font peser les armes de destruction massive. Aucun pays ou groupe de pays ne peut à lui seul y apporter une réponse. Ces problèmes revêtent donc une dimension mondiale et appellent sans plus attendre une réponse concertée de la part de tous les pays, qu'ils soient ou non techniquement développés.

2. Définition des concepts fondamentaux en matière de sécurité de l'information, notamment les interférences illicites dans les systèmes télématiques ou l'utilisation illégale de ces systèmes

3. On trouvera ci-après la définition de certains concepts fondamentaux :

a) *Interférence illicite ou intrusion non sanctionnée*. i) Interférence qui n'est pas le fait d'un gouvernement; ii) interférence sanctionnée par les gouvernements, mais qui ne tombe pas sous le coup du régime international ou des protocoles existant en matière de sécurité de l'information;

b) *Interférence licite*. Interférence commanditée par un gouvernement et prévue par les traités internationaux ou s'inscrivant dans le cadre du régime international ou des protocoles relatifs à la sécurité de l'information;

c) *Utilisation non sanctionnée de l'information*. i) Utilisation d'informations publiques ou privées obtenues soit illégalement soit légalement, sans obtention préalable de l'autorisation des détenteurs de ces informations; ii) utilisation d'informations publiques ou privées présentant un intérêt crucial obtenues soit illégalement soit légalement par des entités gouvernementales à des fins personnelles, ne recoupant pas celles des pouvoirs publics; iii) utilisation d'informations publiques ou privées présentant un intérêt crucial obtenues soit illégalement soit légalement par des entités gouvernementales, sans que le cas ait été prévu dans le cadre d'un régime international, de protocoles relatifs à la sécurité de l'information ou de tous autres loi et traité internationaux;

d) *Utilisation illégale des systèmes télématiques*. i) Utilisation des ressources télématiques, y compris les infrastructures, dans l'intention de nuire; ii) toute utilisation non sanctionnée de l'information;

e) *Ressources informatiques*. Données brutes ou ayant fait l'objet d'un traitement (statistiques, faits, chiffres, dossiers, etc.), logiciels, matériel informatique

(ordinateurs individuels, ordinateurs portables, numériseurs et autres types de technologies nouvelles et avancées), technologies de l'information et moyens connexes (tours d'émission, antennes paraboliques orientables, tours et bâtiments de contrôle), spécialistes des technologies de l'information (programmeurs, analystes fonctionnels, etc.), réseaux et systèmes informatiques (Internet);

f) *Armes informatiques*. Ressources informatiques spécialement mises au point et créées dans le cadre de la guerre informatique ou aux fins de provoquer des dommages, de semer la confusion, de prendre le dessus ou de commettre des actes de malveillance;

g) *Guerre informatique*. Activités visant à obtenir la supériorité dans le domaine informatique au moyen de mesures visant à exploiter, altérer, détruire, fausser ou dénaturer l'information et les fonctions connexes dont dispose l'ennemi; ii) mesures prises pour protéger ses propres ressources et systèmes télématiques; iii) activités par lesquelles on se sert de ses propres ressources et systèmes télématiques pour servir certains desseins et intérêts, par exemple aux fins d'une « guerre cybernétique » (guerre informatique livrée dans le cadre de la défense ou à des fins militaires) ou « guerre sur l'Internet » (guerre informatique livrée à l'échelle plus vaste de la société);

h) *Terrorisme informatique*. Actes terroristes visant à porter atteinte à la sécurité de l'information;

i) *Crime cybernétique ou crime informatique*. i) Acte délictueux dans lequel interviennent certains éléments touchant la sécurité de l'information; ii) acte de malveillance dirigé contre des ressources informatiques (par exemple, technovandalisme, intrusion informatique, utilisation des techniques de superzapping); iii) toute interférence illicite ou intrusion non sanctionnée;

j) *Cyberdélinquant/technodélinquant*. i) Individu commettant des actes qui violent les régimes internationaux ou les protocoles relatifs à la sécurité de l'information; ii) individu dont les actes délictueux ont eu trait à la sécurité informatique ou ont reposé sur celle-ci; iii) individu jugé coupable d'avoir commis à maintes reprises des actes visant les ressources informatiques (une exception devrait être faite en faveur des mineurs pour éviter qu'ils ne soient condamnés comme cyberdélinquants);

k) *Colonialisme informatique*. i) Actes perpétrés par un ou plusieurs États afin de s'imposer et de prendre le dessus dans le domaine de l'information, empêcher l'accès aux technologies de l'information les plus récentes et créer une situation où les autres pays deviennent de plus en plus dépendants dans le domaine des technologies de l'information; ii) actes expansionnistes dans le domaine de l'information et instauration d'un monopole sur l'information et les infrastructures de communication appartenant à un autre pays, qui débouchent sur une situation de dépendance pour les uns et de domination pour les autres;

l) *Pays techniquement développés*. Pays dont les activités économiques reposent à plus de 50 % sur des systèmes informatiques; ii) peut s'employer plus généralement pour désigner les pays développés.

3. Teneur des principes visés au paragraphe 2 de la résolution 55/28 tendant à renforcer la sécurité des systèmes télématiques mondiaux

4. La proposition tendant à établir un régime international en matière de sécurité de l'information revêt à l'heure actuelle une importance cruciale. L'objectif devrait être de rendre responsables de leurs actes les États qui enfreignent les protocoles relatifs à la sécurité de l'information. Il conviendrait aussi de ménager un équilibre entre les pays techniquement développés et ceux qui ne le sont pas. Dans le cadre du régime international, on devrait prendre en compte le cas des pays techniquement développés qui à leur façon « interfèrent » déjà avec les pays défavorisés. En dernier lieu, il importerait de faire de « l'application des lois » un élément central du renforcement de la sécurité internationale de l'information. Dans la pratique, on pourrait créer un centre international chargé, d'une part, de coordonner les activités menées par les services responsables de l'application des lois dans les différents pays aux fins de rechercher les suspects et, d'autre part, d'aider les pays dans le cadre d'activités nationales.

Suède*

[Original : anglais]
[26 juin 2001]

1. À la cinquante-cinquième session de l'Assemblée générale des Nations Unies, les États membres de l'Union européenne ont appuyé la résolution 55/28, intitulée « Les progrès de la téléinformatique dans le contexte de la sécurité internationale ». Les États membres de l'Union européenne souhaitent apporter une réponse commune au paragraphe 3 de la résolution, qui invite les États Membres de l'Organisation des Nations Unies à communiquer leurs vues et observations au Secrétaire général.

1. Examen général des questions relatives à la sécurité de l'information

2. Les technologies de l'information et des communications facilitent grandement la libre circulation de l'information et ont d'importantes retombées sur les individus, les entreprises et les pouvoirs publics de par le monde. Elles contribuent à l'épanouissement de la démocratie et de la liberté d'expression et au renforcement de la société civile. L'Union européenne estime qu'il faut promouvoir et garantir le développement des technologies de l'information et des communications, et défendre le principe de la liberté de l'information. Elle est consciente du risque d'interférence illicite et d'utilisation illégale qui pèse sur les systèmes télématiques, l'intégrité des infrastructures sous-tendues par l'information et l'information détenue par les particuliers, les entreprises, les établissements d'enseignement, les institutions médicales, les organisations du secteur privé et les pouvoirs publics.

3. Assurer la sécurité de l'information et des réseaux consiste à identifier de manière fiable les expéditeurs et les destinataires, à protéger l'information contre tout changement et accès illicites et à garantir l'accès dans des conditions de fiabilité au matériel, aux services et à l'information.

4. Assurer la sécurité de l'information consiste aussi à protéger l'information ayant trait aux capacités militaires et à d'autres aspects de la sécurité nationale. Une protection insuffisante de l'information et des systèmes télématiques cruciaux peut

* Au nom des États membres de l'Union européenne qui sont membres de l'Organisation des Nations Unies.

représenter un danger pour la sécurité internationale.

2. Teneur éventuelle des principes internationaux visant à renforcer la sécurité des systèmes télématiques mondiaux

5. L'Union européenne souhaiterait tout d'abord souligner que si la coopération internationale est fondamentale pour faire face aux problèmes naissants et complexes liés à la sécurité de l'information, chaque pays a avant tout le droit et le devoir de protéger ses propres ressources en matière d'information et de systèmes télématiques.

6. De l'avis de l'Union européenne, certains risques ont un caractère transfrontière et les technologies qui facilitent les attaques contre les systèmes télématiques sont largement disponibles. L'économie de tous les pays repose sur la libre circulation de l'information et l'usage des technologies de l'information à des fins pacifiques. Toute action préventive visant à contenir des attaques criminelles et terroristes, y compris afin de faire face aux menaces pesant sur la sécurité internationale, doit être entreprise dans le respect de la protection de l'information et des systèmes sous-tendus par l'information.

7. Plusieurs initiatives multilatérales sont déjà consacrées à la coopération internationale dans le domaine de la sécurité de l'information. Elles sont notamment le fait du Conseil de l'Europe; du dixième Congrès des Nations Unies pour la prévention du crime et le traitement des délinquants, qui s'est tenu du 10 au 17 avril 2000 (voir A/CONF.187/15); de la Commission pour la prévention du crime et la justice pénale, qui relève de l'ONU; du Groupe de travail spécial sur l'informatique du Conseil économique et social; du Groupe d'étude sur les technologies de l'information et des télécommunications, qui relève de l'ONU; de l'Organisation de coopération et de développement économiques; de l'Union internationale des télécommunications; des groupes chargés de la lutte contre la cybercriminalité dans le cadre du G-8; et de l'Organisation des États américains.

8. L'Union européenne juge que les États Membres de l'Organisation devraient suivre les travaux des organismes et organes susmentionnés aux fins d'évaluer, le moment voulu, le type de mesures pratiques qui pourraient s'avérer utiles dans ce domaine. Elle considère que la Première Commission n'est pas l'organe de l'Assemblée générale le plus approprié pour examiner les questions relatives à la sécurité de l'information. Dans la mesure où ces questions concernent en grande partie des domaines autres que le désarmement et la sécurité internationale, l'Union européenne estime qu'il serait plus judicieux de confier l'examen de certains aspects du problème à d'autres comités.